



Recursos capítulo 3

Unidad didáctica 3.
Relación entre la Inteligencia Artificial (IA) y la ciberseguridad, que es la estafa del CEO o (BEC) y su relación con la IA, otros tipos de estafas mediante IA y posibles antídotos para estas estafas.



@estudioprompt

ÍNDICE

Introducción	5
1.1 Presentación.....	5
1.2 Objetivos de aprendizaje.....	5
2. Ciberseguridad y ciberdelitos.....	8
2.1 La Inteligencia Artificial y la Ciberseguridad.....	8
2.3 Inteligencia Artificial y suplantación de identidad.....	9
3. La Estafa del CEO y el Fraude BEC.....	11
3.1 ¿Qué es la estafa del CEO?.....	11
3.2 La IA en la estafa del CEO.....	14
4. Otros Tipos de Estafas a empresas Mediante IAs.....	17

4.1 Fraude de las facturas y estafa de inversión	17
4.2 Fraudes de suplantación bancaria y los deepfakes	18
5. Posibles Antídotos para Estafas con Inteligencia Artificial.....	19
5.1 Educación	19
5.2 Protocolos de verificación	20
5.3 Protocolos de Cambios.....	20
5.4 Limitación de información pública.....	21
5.5 Actualización de seguridad del sistema.....	21
6. Cierre.....	22
6.1 ¿Qué has aprendido?.....	22

1. Introducción

1.1 Presentación

Te damos la bienvenida a la unidad didáctica 3. “Relación entre la Inteligencia Artificial (IA) y la ciberseguridad, que es la estafa del CEO o (BEC) y su relación con la IA, otros tipos de estafas mediante IA y posibles antídotos para estas estafas.”

1.2 Objetivos de aprendizaje

Los objetivos de aprendizaje de esta unidad didáctica son:

- a. Interiorizarse en el ámbito de la ciberseguridad, adquiriendo un entendimiento profundo de cómo las nuevas tecnologías, especialmente la Inteligencia Artificial (IA), están impactando y transformando el panorama de la seguridad digital.
- b. Comprender en detalle qué significa la "Estafa del CEO" o "BEC" (Business Email Compromise), identificando sus características principales, modus operandi y las implicaciones que tiene en el mundo empresarial y financiero.
- c. Analizar cómo la IA puede ser utilizada tanto en la detección y prevención de ciberataques, como en la potenciación de estafas y amenazas cibernéticas.

- d. Evaluar las diferentes modalidades de estafas potenciadas por la IA, incluyendo pero no limitado a fraudes de facturas, estafas de inversión y suplantaciones bancarias.
- e. Identificar las técnicas y herramientas de IA, como los deep fakes, que están siendo utilizadas por ciberdelincuentes para crear contenidos falsos y engañosos.
- f. Reflexionar sobre la importancia de la educación y la prevención como principales herramientas de defensa contra las estafas y amenazas potenciadas por la IA.
- g. Desarrollar habilidades críticas para reconocer y responder adecuadamente ante posibles intentos de estafas o ataques

cibernéticos en su entorno profesional y personal.

h. Explorar soluciones y estrategias recomendadas para fortalecer la ciberseguridad en la era de la IA, incluyendo protocolos de verificación, actualizaciones de sistemas y educación continua.

2. La Inteligencia Artificial y la Ciberseguridad

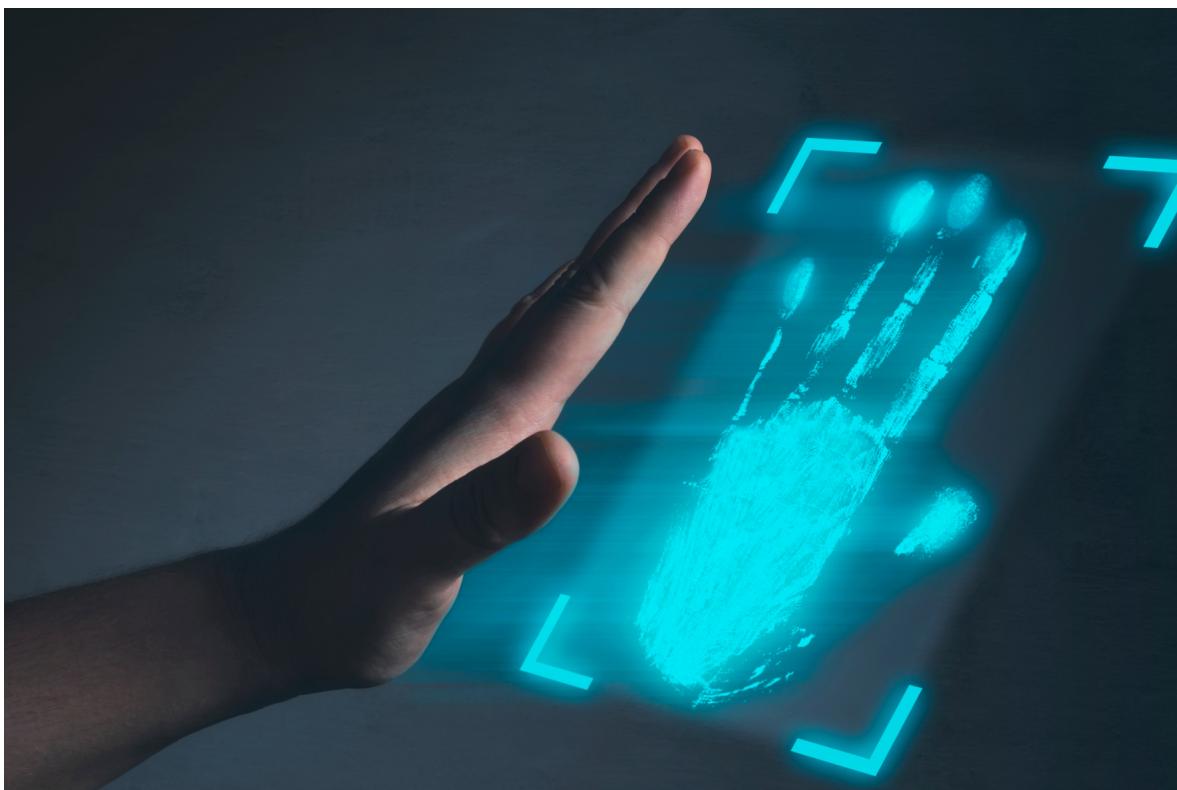
2.1 La IA en los ciberdelitos



La digitalización ha traído consigo una evolución en los ciberdelitos. La IA se ha convertido en una herramienta poderosa tanto para los ciberdelincuentes como para los defensores de la ciberseguridad. La IA puede ser utilizada para detectar amenazas y responder a ellas de manera más eficiente. Sin embargo, también puede ser empleada por los

cibercriminales para llevar a cabo ataques más sofisticados

2.2 Inteligencia Artificial y suplantación de identidad.



La suplantación de identidad es una de las tácticas más antiguas en el

libro de los ciberdelincuentes. Sin embargo, con la IA, estos ataques pueden ser mucho más convincentes. Al analizar la forma en que una persona escribe o habla, la IA puede imitar ese estilo, haciendo que los intentos de suplantación sean casi indistinguibles de los mensajes reales.

Una decena de caras generadas con IA pueden suplantar la identidad | Business Insider España

3. La Estafa del CEO y el Fraude BEC.

3.1 ¿Qué es la estafa del CEO?



La estafa del CEO, la cual cuenta con muchas modalidades donde la más conocida es BEC (Business Email Compromise), es básicamente una suplantación de identidad de tomadores de decisiones, una táctica que ha ganado popularidad en los últimos años. En este tipo de estafa, los ciberdelincuentes se hacen pasar por altos ejecutivos y solicitan transferencias de dinero o

información confidencial. A menudo, estos correos electrónicos son tan convincentes que incluso los empleados más experimentados pueden ser engañados.

Otra modalidad de la misma estafa es Una tercera persona, el estafador, conocido como (el hombre en el medio), interfiere en las conversaciones mantenidas mediante correo electrónico entre dos empresas o corporaciones para sus relaciones comerciales o de servicios. El estafador suplanta la identidad de una de las empresas y envía un correo electrónico falso, simulando los logotipos y el estilo de los originales, comunicando un cambio de cuenta bancaria donde realizar los pagos. Si

la empresa pagadora no confirma directamente con la otra parte ese cambio de número, a partir de ese momento realizará los pagos a una cuenta corriente controlada por el timador. Así, el dinero nunca llega a su perceptor legítimo, Debido a la presión, la urgencia y el respeto por la autoridad, los empleados u otros ejecutivos acceden

3.2 La IA en la estafa del CEO.



La IA puede potenciar la estafa del CEO de varias maneras. Por ejemplo, puede analizar correos electrónicos previos para imitar el estilo de escritura del CEO. Además, puede identificar a los empleados que tienen acceso a información financiera y que podrían ser objetivos para la estafa.

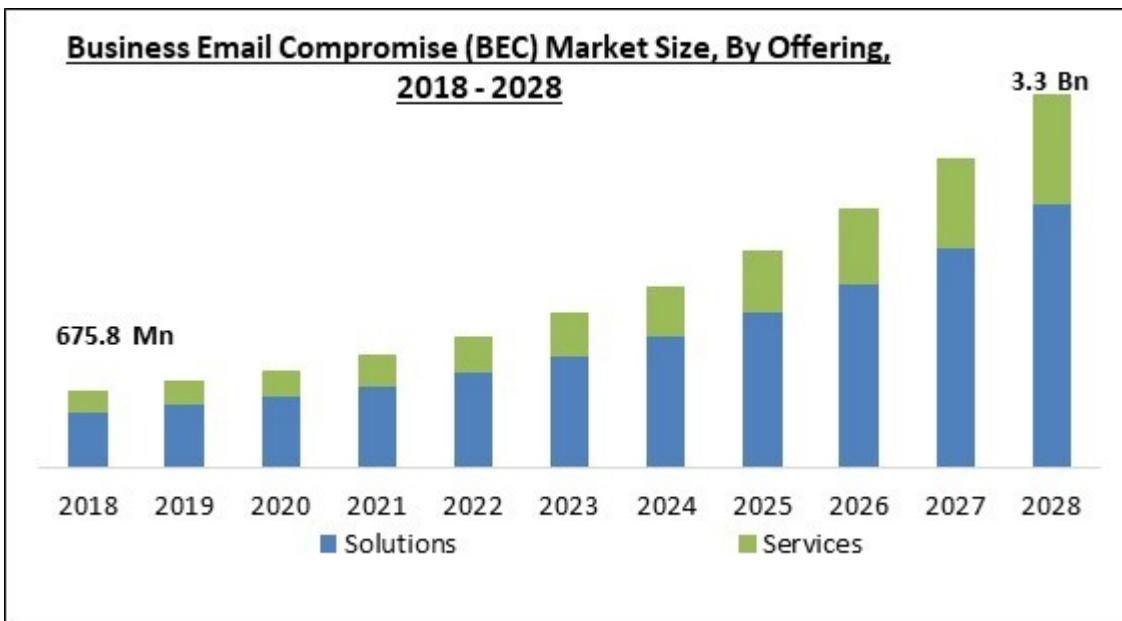
Lo alarmante de estas estafas es que la IA es una especialista en

suplantación de identidad y puede jugar un papel significativo en hacerlas más efectivas. Las IAs pueden ser entrenadas para analizar y aprender de las comunicaciones anteriores, imitando su estilo de escritura, su vos, incluso se puede generar un video para confundir, para hacer que las comunicaciones sean aún más convincentes. También pueden identificar a los empleados que tienen acceso a las cuentas de la empresa y pueden ser más susceptibles al engaño.

Según un estudio realizado en Dublín en 2022 Se espera que el tamaño del mercado Global Business Email Compromise (BEC) alcance los \$ 3.3 mil millones para 2028, aumentando a un crecimiento del mercado de 19.0%

durante el período de pronóstico.
dejamos el link en la descripción

Global Business Email Compromise (BEC) Market Size, Share & Industry Trends Analysis Report By Offering (Solutions and Services), By Deployment Mode, By Organization Size (Large Enterprises and SMEs), By Vertical, By Regional Outlook and Forecast, 2022 - 2028



4. Otros Tipos de Estafas a empresas Mediante IAs.

4.1 Fraude de las facturas y estafa de inversión

El fraude de facturas es similar a la estafa BEC. Los ciberdelincuentes se hacen pasar por proveedores y solicitan cambios en los detalles de pago. La estafa de inversión, por otro lado, implica promesas de grandes retornos con poco o ningún riesgo. La IA puede hacer que estas estafas sean más convincentes al proporcionar detalles falsos pero plausibles.



4.2 Fraudes de suplantación bancaria y los deep fakes .

Los fraudes de suplantación bancaria buscan obtener acceso a cuentas bancarias. Los deep fakes, por otro lado, son videos o audios generados por IA que parecen reales. Estos pueden ser utilizados para suplantar la identidad de alguien y engañar a las personas para que realicen

acciones que de otra manera no harían.

5. Posibles Antídotos para Estafas con Inteligencia Artificial.

5.1 Educación.



La educación es la primera línea de defensa contra las estafas. Es esencial que los empleados estén informados

sobre las diferentes tácticas que los ciberdelincuentes pueden usar.

5.2 Protocolos de verificación .

Establecer protocolos de verificación puede ayudar a prevenir estafas. Por ejemplo, cualquier solicitud de transferencia de dinero debe ser verificada por dos personas.

5.3 Protocolos de Cambios.

Antes de hacer cambios en los detalles de pago o en la información confidencial, es esencial seguir un protocolo establecido para verificar la autenticidad de la solicitud.



5.4 Limitación de información pública.

Limitar la cantidad de información disponible públicamente puede reducir el riesgo de suplantación de identidad y otras estafas.

5.5 Actualización de seguridad del sistema.

Mantener los sistemas actualizados y protegidos con las últimas medidas

de seguridad es esencial para protegerse contra las amenazas.



6. Cierre

6.1 Punteo de lo aprendido

- Introducción a la Ciberseguridad y la IA: La era digital ha traído consigo desafíos y oportunidades en el ámbito de la ciberseguridad, y la Inteligencia Artificial juega un papel crucial en este escenario.
- IA y Ciberseguridad: La IA ofrece herramientas poderosas para detectar y prevenir amenazas cibernéticas, pero también puede ser utilizada por cibercriminales para perpetrar ataques más sofisticados.
- Suplantación de identidad potenciada por IA: La IA puede imitar estilos de escritura y comunicación, lo que puede llevar a ataques de suplantación de identidad más convincentes.
- Estafa del CEO o BEC: Una táctica donde los cibercriminales se hacen pasar por altos ejecutivos

para solicitar transferencias de dinero o información confidencial. La IA puede potenciar esta estafa al imitar el estilo de comunicación del CEO.

- Otros tipos de estafas mediante IA: Además de la estafa del CEO, existen otros tipos de fraudes como el fraude de facturas, estafa de inversión, y fraudes de suplantación bancaria. Los deepfakes, generados por IA, pueden ser utilizados para suplantar identidades en videos o audios.
- Antídotos contra estafas con IA: La educación y la conciencia son esenciales. Establecer protocolos de verificación, limitar la información pública y mantener los sistemas actualizados son

medidas proactivas para combatir las amenazas.